COVARIANTS OF BINARY MODULAR GROUPS

By Oliver Edmunds Glenn

Department of Mathematics, University of Pennsylvania

Communicated by E. H. Moore, January 30, 1919

To transform the general case of a binary quantic

$$f_m = (a_0, a_1, \ldots, a_m \between x_1, x_2)^m,$$

by substituting for its variables

$$x_1 = \lambda_1 x_1' + \mu_1 x_2', \; x_2 = \lambda_2 x_1' + \mu_2 x_2',$$

where the coefficients of the transformation are least positive residues of a prime number p, is to generate an infinitude of binary forms associated with f_m, which are invariants of the linear modular group G of order $(p^2 - p) \times (p^2 - 1)$, on the variables x_1, x_2.

Much difficulty has been encountered by those who have investigated these invariants, both as to methods of generating complete systems and as to proofs of their finiteness. This paper is in the form of a summary of the present writer's research on this problem. It contains an outline of a method of construction of the formal modular covariants which has a measure of generality,—and which has proved to be definitive,—at least for particular moduli. Secondly we give, in explicit form, the finite modular systems of the cubic (mod 2) and of the quadratic (mod 3). Phases of the formal modular theory not mentioned in this paper are treated in articles by the present writer, referred to at the end of this paper, and in Dickson's Madison Colloquium lectures.

1. Modular convolution.—If $S(a_0, a_1, \ldots)$ is any modular seminvariant of f_m which satisfies a certain pair of conditions,[5c] and $a_0', a_1', \ldots$ are the coefficients of the transformed of f_m by means of

$$x_1 = x_1 + tx_2', \; x_2 = x_2'; \; (t \text{ any residue mod } p),$$

then, S' being the conjugate to S under the substitution $(a_0a_2)(a_1)$,

$$S'(a_0', a_1', \ldots) \equiv S(a_0, \ldots)t^{p-1} + S_1 t^{p-2} + \ldots + S_{p-1} \pmod{p}, \quad (1)$$

written with homogeneous variables x_1, x_2, instead of t, is a formal covariant modulo p. When this principle is applied in the case of the seminvariant leading coefficient of the covariant K_ν:

$$K_\nu = C_0 x_1^\nu + C_1 x_1^{\nu-1} x_2 + \ldots + C_\nu x_2^\nu,$$

where ν is a number of the form

$$\nu = (sp - \nu')(p - 1) = \sigma(p - 1),$$

there results a covariant[6]

$$[K_\nu] = [C_0 + (K_\nu)]\, x_1^{p-1} + \sum_{r=0}^{p-2} \sum_{s=0}^{\sigma-1} C_{\nu - s(p-1)-r}\, x_1^{p-r-1} x_2^r, \qquad (2)$$

where (K_ν) is the pure invariant

$$(K_\nu) = C_{p-1} + C_{2(p-1)} + \ldots + C_{(\sigma-1)(p-1)}. \qquad (3)$$

Now if we form the product of any two binary forms, as of f_m and

$$g_n = (b_0, b_1, \ldots, b_n)(x_1, x_2)^n \; (m \geqq n),$$

where $m + n$ is a number of the form $\sigma\,(p-1)$, and construct the formulas analogous to (2), (3) for the result, we get

$$(f_m g_n) = \sum_{i=0}^{j(p-1)} \sum_{j=1}^{\sigma-1} a_i b_{j(p-1)-i},$$

$$[f_m g_n] = [a_0 b_0 + (f_m g_n)]\, x_1^{p-1} + \sum_{r=0}^{p-2} \sum_{s=0}^{\sigma-1} \sum_{i=0}^{t} a_i b_{(\sigma-s)(p-1)-r-i}\, x_1^{p-r-1} x_2^r$$

$$\{t = (\sigma - s)(p-1) - r\}.$$

This process of constructing the concomitants $(f_m g_n)$, $[f_m g_n]$ from the product $f_m \cdot g_n$ is analogous to transvection and symbolical convolution in the theory of algebraic concomitants.

An example of the covariant (1) is obtained from the following seminvariant[3] of a quadratic form f_2:

$$S = a_0^{p-1} a_1 - a_1^p.$$

This seminvariant satisfies the two necessary and sufficient conditions that it may be the leading coefficient of a covariant, viz., of [5c]

$$C_1 = (a_0 x_1 + a_1 x_2)^p - (a_0 x_1 + a_1 x_2)(a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2)^{p-1}, \qquad (4)$$

where powers of x_1, x_2 are to be reduced by Fermat's theorem.

2. *Concomitant scales.*—If K is any modular covariant of order $(rp - \nu) \times (p-1) = m$, then by application, to K, of the latter of the two modular invariantive operators [5b]

$$E = a_0^p \frac{\delta}{\delta a_0} + a_1^p \frac{\delta}{\delta a_1} + \ldots + a_m^p \frac{\delta}{\delta a_m},$$

$$\omega = x_1^p \frac{\delta}{\delta x_1} + x_2^p \frac{\delta}{\delta x_2},$$

there is obtained a set or scale of $\mu = p + \nu + 2$ concomitants

$$(K),\ \omega^\lambda [K]\ (\lambda = 0, 1, \ldots, p-1),\ \omega^t K\ (t = 0, 1, \ldots, \nu). \qquad (5)$$

This set, which we call a *μ-adic* scale[6] for K, is analogous to the set obtainable by convolution from a symbolical algebraic covariant

$$\Pi\,(ab)\, a_x^p\, b_x^q\, c_x^r \cdots.$$

A scale of modular concomitants is said to be *complete* when it contains all invariants and covariants of the first degree in the coefficients of K which can be obtained from K by empirical or modular invariantive processes, i.e. a μ-*adic* scale is complete when it constitutes a fundamental system of first degree concomitants of K. Thus we find that we are able to construct a complete modular system of a form f_m by a process of passing from a complete scale for f_m of the first degree to scales derived from covariants of f_m of degree > 1.

3. A complete system of the quadratic, modulo 3.—I have proved that the following eighteen quantics constitute a complete formal system modulo 3 of f_2; the proof resting primarily upon the fact that, when $p = 3$, every covariant is of even order, and hence the μ-*adic* scale (5) is complete:

$$\begin{gathered} f_2,\ C_1,\ [f_2^2],\ [f_2C_1],\ [f_2^2C_1],\ Ef_2, \\ \omega f_2,\ \omega C_1,\ \omega[f_2^2],\ \omega Ef_2,\ \omega^2 f_2,\ \omega^2 C_1, \\ L,\ Q,\ (f_2^2),\ ([f_2^2]^2),\ (C_1Ef_2),\ \Gamma; \end{gathered} \tag{6}$$

where[3] $\Gamma = (a_0 + a_2)(2a_0 + 2a_1 + a_2)(2a_0 + a_1 + a_2)$, and L, Q are the functions to which the universal covariants of the group $G_{(p^2-p)(p^2-1)}$ reduce when $p = 3$. These covariants are[3]

$$L = x_1^p x_2 - x_1 x_2^p,\ Q = (x_1^{p^2} x_2 - x_1 x_2^{p^2})/L.$$

The last four quantics in the system (6) are pure invariants and constitute a complete system of invariants of f_2 modulo 3. This set of invariants was first derived by Dickson. The orders of the forms (6) range from 0 to 6 and the degrees from 0 to 6.

4. A complete system of the cubic, modulo 2.—When $p = 2$ the μ concomitants (5) do not form a complete scale. Every form of order > 3 is reducible[5e] modulo 2 in terms of invariants of the first degree in its coefficients and of its covariants of orders 1, 2 and 3. If K_ν is the covariant shown in §1 we have ($p = 2$),

$$\begin{aligned} (K_\nu) &= C_1 + \ldots + C_{\nu-1}, \\ [K_\nu] &= [C_0 + (K_\nu)]x_1 + [(K_\nu) + C_\nu]x_2. \end{aligned}$$

These, and the additional covariant

$$\{K_\nu\} = C_0 x_1^2 + (K_\nu)x_1x_2 + C_\nu x_2^2,$$

exist for all orders ν. When ν is odd there exists also a cubic covariant[5c]

$$\{\overline{K_\nu}\} = C_0 x_1^3 + I_1 x_1^2 x_2 + I_2 x_1 x_2^2 + C_\nu x_2^3,$$

where I_1, I_2 are definite linear expressions in $C_1, \ldots, C_{\nu-1}$ such that[5d]

$$I_1 + I_2 \equiv (K_\nu)\,(\text{mod } 2).$$

These concomitants, and their polars by $\omega = x_1^2 \frac{\delta}{\delta x_1} + x_2^2 \frac{\delta}{\delta x_2}$, form a complete scale for K_ν.

A fundamental system of formal covariants of f_3 modulo 2 consists of the following twenty quantics;[5d] where we abbreviate by H the algebraic hessian of f_3, and

$$t = H + (f_3)\{f_3\},\ l = Q[H] + f_3\ (f_3),$$

and in which L, Q are the universal covariants of the group G_6:

$$f_3, H, [f_3], \{f_3\}, Ef_3, E[f_3], \{f_3t\}, \{Pt\}, [f_3t],$$
$$[Ef_3 \,.\, t], \{\overline{f_3t}\}, \{\overline{tEf_3}\}, [Ql], L, Q,$$
$$(f_3), (H), (tf_3), (tEf_3), I.$$

The invariant I, which is not represented as belonging to any scale, is

$$I = a_0^2 + a_0a_3 + a_3^2 + (a_0 + a_3)(f_3).$$

The orders of the forms in this system range from 0 to 3, and their degrees from 0 to 4.

The proofs of the existence of $\{\overline{K_\nu}\}$ and of $[K_\nu]$ involve certain remarkable congruential properties of the binomial coefficients.[6]

Reduction methods rest largely upon the fact that two modular covariants of the same order and led by the same seminvariant, while not identical as a rule, are necessarily congruent to each other moduli $L (= x_1^p x_2 - x_1 x_2^p)$, and p. Thus a covariant is not uniquely determined by its seminvariant leading coefficient as is the case with algebraic covariants. Another noteworthy general fact is that of the existence of covariants whose leading coefficients are modular invariants.

[1] Hurwitz, A., *Archiv. Math. Phys., Leipzig*, (Ser. 3), **5**, 1903, (17).

[2] Dickson, L. E., *Trans. Amer. Math. Soc.*, **10**, 1909, (123); **12**, 1911, (75); **14**, 1913, (290); and **15**, 1914, (497); *Amer. J. Math., Baltimore*, **31**, 1909; etc.

[3] Dickson, *Madison Colloquium Lectures*, 1913.

[4] Miss Sanderson, *Trans. Amer. Math. Soc.*, **14**, 1913.

[5] Glenn, O. E., (a) *Amer. J. Math.*, **37**, 1915, (73); (b) *Bull. Amer. Math. Soc., New York*, **21**, 1915, (167); (c) *Trans. Amer. Math. Soc.*, **17**, 1916, (545); (d) **19**, 1918, (109); (e) *Ann. Math., Princeton*, **19**, 1918, (201).

[6] A paper containing a portion of the general theory here mentioned and the derivation of the system of the quadratic modulo 3, as well as certain other developments, is to appear in *Trans. Amer. Math. Soc.*